

ABSTRACT
Virtual Private Networks

A secure communication method for allowing a mobile host 1 to communicate with a correspondent host 4 over a Virtual Private Network. The method comprises negotiating one or more Security Associations (SAs) between the mobile host 1 and a correspondent host 4 of a Virtual Private Network (VPN). Subsequently, a communication is initiated between the mobile host 1 and a SG 3 and an authentication certificate sent to the SG 3, the certificate containing at least the identity of a SA which will be used for subsequent communication between the mobile host and the correspondent host. Data packets can then be sent from the mobile host 1 to the correspondent host 4 using the identified SA, via the SG 3. However, the data packets are forwarded by the SG 3 to the correspondent host 4 only if they are authenticated by the SG 3.

Figure 1

2025 RELEASE UNDER E.O. 14176